

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation,

Plaintiff and Counterclaim-Defendant,

v.

INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation, and SYMANTEC CORPORATION, a Delaware corporation,

Defendants and Counterclaim- Plaintiffs.

Civil Action No. 04-CV-1199 (SLR)

PUBLIC VERSION

THIS DOCUMENT CONTAINS MATERIALS WHICH ARE CLAIMED TO BE CONFIDENTIAL OR RESTRICTED CONFIDENTIAL - CONFIDENTIAL SOURCE CODE AND COVERED BY A PROTECTIVE ORDER. THIS DOCUMENT SHALL NOT BE MADE AVAILABLE TO ANY PERSON OTHER THAN THE COURT AND OUTISDE COUNSEL OF RECORD FOR THE PARTIES

DECLARATION OF GEOFFREY M. GODFREY IN SUPPORT OF DEFENDANT'S JOINT REPLY MOTION FOR SUMMARY JUDGMENT REGARDING INVALIDITY

Original Dated: July 10, 2006

REDACTED VERSION: July 19, 2006

I, Geoffrey M. Godfrey, declare as follows:

1. I am a member of the law firm of Day Casebeer Madrid & Batchelder LLP, counsel for Defendant Symantec Corporation. I am admitted to practice law before all courts of the State of California.

2. I make this declaration of my own personal knowledge. If called to testify as to the truth of the matters stated herein, I could and would do so competently.

3. Attached hereto as Exhibit QQ is a true and correct copy of Plaintiff SRI's Second Supplemental Responses to Defendant Symantec's First Set of Interrogatories [Nos. 1-12].

4. Attached hereto as Exhibit RR is a true and correct copy of selected pages of the 03/09/2006 and 03/10/2006 Deposition of Phillip Porras (hereinafter "Porras Tr.") and the 03/30/2006 30(b)(6) Deposition of Phillip Porras (hereinafter "Porras 30(b)(6) Tr.").

5. Attached hereto as Exhibit SS is a true and correct copy of selected pages of the 05/26/2006 and 05/29/2006 Deposition of George Kesidis (hereinafter "Kesidis Tr.").

6. Attached hereto as Exhibit TT is a true and correct copy of selected pages of the 03/23/2006 Deposition of Alfonso Valdes (hereinafter "Valdes Tr.").

7. Attached hereto as Exhibit UU is a true and correct copy of selected pages of the 01/27/2006 Deposition of Y. Frank Jou (hereinafter "Jou Tr.").

8. Attached hereto as Exhibit VV is a true and correct copy of selected pages of the 03/31/2006 Deposition of Peter G. Neumann (hereinafter "Neumann Tr.").

9. Attached hereto as Exhibit WW is a true and correct copy of SRI's Supplemental Response to Symantec's Interrogatories Nos. 12 and 15, dated Dec. 15, 2005.

10. Attached hereto as Exhibit XX is a true and correct copy of SRI's Supplemental Response to Symantec's Interrogatories Nos. 1 and 12 (First Set of Interrogatories), 13 and 15 (Second Set of Interrogatories), dated May 05, 2006.

11. Attached hereto as Exhibit YY is a true and correct copy of pages 19-20 of R.

Bace, INTRUSION DETECTION (Macmillan Technical Publishing 2000).

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge.

Dated: July 10, 2006

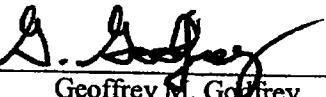
By: 
Geoffrey M. Godfrey

EXHIBIT QQ

**EXHIBIT REDACTED
IN ITS ENTIRETY**

EXHIBIT RR

**EXHIBIT REDACTED
IN ITS ENTIRETY**

EXHIBIT SS

**EXHIBIT REDACTED
IN ITS ENTIRETY**

EXHIBIT TT

**EXHIBIT REDACTED
IN ITS ENTIRETY**

EXHIBIT UU

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

C.A:04-1199 (SLR)

SRI INTERNATIONAL, INC.,)
a California Corporation)
Plaintiff and)
Counterclaim Defendant,)
v.)
INTERNET SECURITY SYSTEMS, INC.,)
a Delaware Corporation, INTERNET)
SECURITY SYSTEMS, INC., a Georgia)
Corporation, and SYMANTEC)
CORPORATION, a Delaware)
Corporation,)
Defendants and)
Counterclaim-Plaintiffs.)
- - - - -

COPY

VIDEOTAPED DEPOSITION

OF

Y. FRANK JOU

At Raleigh, North Carolina
January 27, 2006 - 9:53 a.m.

Reported by:
Debra D. Bowden

capitalreporting

PO Box 97696
Raleigh, NC 27624

www.capreporting.com

8360 Six Forks Road
Suite 101
Raleigh, NC 27615

919.398.7775 ph
919.398.7741 fax

capreporting@aol.com

171

1 fruit even though if the time or resource
2 is allowed at that point in time.
3 Q. If you go back to the architecture
4 document, J18, on page 3.
5 A. Page 3. Okay.
6 Q. And if you go to Section 2.1.
7 A. Um-hmm.
8 Q. And you go to the third paragraph.
9 A. Um-hmm.
10 Q. The middle of it. And you say, "While it
11 is not within the scope of this project, we
12 expect that the detection analysis
13 functions implemented in the local
14 subsystem can be extended to a global level
15 and correlate intrusion events among
16 several routers." Do you see that?
17 A. Um-hmm.
18 Q. And then it goes on to say, "The management
19 capability which is based on SNMP framework
20 can logically be further extended among
21 management nodes in a hierarchical fashion
22 to establish a status map for an autonomous
23 system."
24 A. Um-hmm.

172

1 Q. Now, while your DARPA project was limited
2 in time and funding, did you create the
3 design such that it could be extended in
4 this hierarchical fashion?

5 A. I would not say created, because the SNMP
6 network by its nature is to monitor remote
7 system.

8 Q. Um-hmm.

9 A. And be able to reflect a healthy -- the
10 healthy -- the status of the network, you
11 know, it's healthy, whether it's healthy or
12 it's, you know, under stress. That was the
13 intent of the SNMP framework. And our
14 thinking at that point in time was to take
15 advantage of this SNMP by the fact that
16 it's able to monitor several systems in a
17 distributive fashion. And you know, the
18 challenge at that point was how do you
19 correlate. I think that was the main
20 technical challenge at that point in time
21 in terms of how do you collect -- collect
22 of the local detection result was not an
23 issue. The issue was how do you come up
24 with the intelligence, how do you correlate

173

1 all the relevant information and be able
2 to, you know, derive a certain logical or
3 reasonable conclusion, and able to, based
4 upon this result, take action accordingly.
5 I think that was the challenge, and the --
6 you know, we did look into that aspect.
7 But however at that point we did not have a
8 very promising, you know, development at
9 that time. At the conclusion of the
10 project. So that was, you know, the open
11 question at that point.

12 Q. And if you just saw the term correlate --

13 A. Um-hmm.

14 Q. -- what would that mean to you?

15 MS. PRESCOTT: Objection to form.

16 A. Correlate means how do you put two or more
17 than two input together and derive
18 meaningful information, or intelligence,
19 out of these different infrastreams of
20 information, and be able to come up with
21 certain rationale or logic that what this,
22 you know, behavior manifests to itself.

23 Probably that's kind of lengthy or
24 wordy, but that's my understanding of this

174

1 word, correlation.

2 MS. MOEHLMAN: Okay, let me go off
3 the record for two minutes.

4 VIDEOGRAPHER: Going off the record,
5 the time is 15:31.

6 (Continuing after recess.)

7 VIDEOGRAPHER: Back on the record,
8 the time is 1534.

9 MS. MOEHLMAN: Thank you very much
10 for your time today. We are concluded.

11 THE WITNESS: Okay. My pleasure.

12 VIDEOGRAPHER: This concludes volume
13 one of the deposition of Y. Frank Jou. The
14 videographer was Bob Collier for the firm
15 of Capital Reporting of Raleigh, North
16 Carolina. The deposition was held at the
17 offices of Smith Moore, Raleigh, North
18 Carolina, on January 27th, 2006. The
19 number of tapes used was three. The time
20 is 15:34.

21 [DEPOSITION CONCLUDED]

22

23

24

EXHIBIT VV

**EXHIBIT REDACTED
IN ITS ENTIRETY**

EXHIBIT WW

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California
Corporation,

Plaintiff,

v.

INTERNET SECURITY SYSTEMS, INC.,
a Delaware corporation, INTERNET
SECURITY SYSTEMS, INC., a Georgia
corporation, and SYMANTEC
CORPORATION, a Delaware corporation,

Defendants.

Case No. 04-1199-SLR

**SRI INTERNATIONAL, INC.'S SUPPLEMENTAL RESPONSE TO
INTERROGATORIES NO. 12 AND NO. 15**

Pursuant to Federal Rules of Civil Procedure 26 and 33, Plaintiff SRI International, Inc. ("SRI") supplements its response to Defendant Symantec Corporation's ("Symantec") Interrogatory No. 12 as follows:

GENERAL OBJECTIONS

SRI incorporates by reference all of its General Objections to Symantec's Interrogatories Nos. 12 and 15.

RESPONSE

INTERROGATORY NO. 12:

For each asserted claim of the asserted patents, describe in detail all evidence of "secondary considerations" that support your contention that the subject matter of the claim is non-obvious under 35 U.S.C. § 103. The term "secondary considerations" in this interrogatory is in accordance with the manner in which it was used in *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). Your description should include an identification of evidence of commercial success, long-felt need, copying by others, attempts by others to solve any problem addressed by the accused patents, and acceptance in the industry or by

the public of any claimed invention.

For each asserted claim your answer should also include an identification of the three SRI employees (excluding attorneys) most knowledgeable about any such evidence of non-obviousness (listed in order from most knowledgeable to least knowledgeable) and an identification of all documents concerning such evidence.

RESPONSE TO INTERROGATORY NO. 12 (AUGUST 29, 2005):

SRI objects to this request on the grounds that it prematurely seeks SRI's contentions and the subject of expert testimony. SRI will abide by the schedule set forth by the Court's to respond fully to this interrogatory.

SRI further states that it will produce documents in its possession regarding any secondary considerations of non-obviousness that SRI is able to locate after a reasonable search and that could be arguably responsive to the request. SRI incorporates information contained in these documents pursuant to Fed. R. Civ. P. 33(d). The person most knowledgeable about the secondary considerations for the patents-in-suit is Peter Neumann.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 12 (OCTOBER 18, 2005):

SRI incorporates by reference its original response to Interrogatory No. 12. SRI provides the following additional information:

Documents with the following bates numbers ranges may contain information responsive to this interrogatory: SRI 000193-003207; SRI 003629-006630; SRI 007864-008974; SRI 016450-017430; SRI 018203-018434; SRI 019552-020262; SRI 027996-028715; SRI 029381-030492; SRI 037164-037391; SRI 044105-044106; SRI 044130-044131; SRI 044193; SRI 044196-044199; SRI 044295; SRI 050529-051726; SRI 053609-053624; SRI 053701-055815; SRI 075959-078987.

SRI further states that discovery in this case is ongoing. SRI reserves the right to supplement this response as additional information and documents become available.

FURTHER SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 12
(NOVEMBER 18, 2005):

SRI incorporates by reference its original and first supplemental response to Interrogatory No. 12. SRI provides the following additional response:

SRI objects to this interrogatory as premature. The identification of secondary considerations of non-obviousness is only required once Symantec has made a *prima facie* showing of obviousness. SRI will provide a further response to this interrogatory at the time the Court's scheduling order has set for providing rebuttal contentions. In the event that Symantec makes an obviousness argument, SRI intends to rely at least on a showing of commercial success and long felt need.

THIRD SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 12
(DECEMBER 15, 2005):

SRI incorporates by reference its previous responses to Interrogatory No. 12. SRI provides the following additional response:

SRI intends to rely on at least the following objective indicia of non-obviousness: commercial success of the accused products, praise in the marketplace (e.g., DARPA), long-felt need, and failure by others. The fact that many other research groups were attempting to create a practical solution to the problem of network intrusion detection, but that none were successful before SRI's inventions (See SRI's Response to Symantec's Invalidity Contentions) is strong evidence of non-obviousness.

INTERROGATORY NO. 15:

Identify each limitation of each claim of each of the asserted patents that SRI contends is not disclosed in the Network NIDES publication.

RESPONSE TO INTERROGATORY NO. 15

SRI objects that the phrase "Network NIDES publication" is vague and ambiguous in that the publication describes a host-based system rather than a network system. SRI objects to this request in that it prematurely seeks SRI's contentions and expert testimony. To the extent that Symantec provides SRI with contentions regarding any assertion that Symantec has about the invalidity of the patents-in-suit in light of the article "*Next-generation Intrusion Detection Expert System (NIDES) A Summary,*" by Debra Anderson, Thane Frivold and Alfonso Valdes, Jan. 27, 1995, SRI will respond according to the procedural schedule the Court has set forth in this litigation.

Subject to, and without waiving the foregoing objections and general objections, SRI states that the claimed inventions of the patents-in-suit are not disclosed in the article "*Next-generation Intrusion Detection Expert System (NIDES) A Summary,*" by Debra Anderson, Thane Frivold and Alfonso Valdes, Jan. 27, 1995.

SRI further states that its investigation is ongoing and that it reserves the right to supplement its response to this interrogatory as appropriate.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 15

SRI incorporates by reference, its previous responses to Interrogatory No. 15 and further states that because Defendants' bear the burden of proof on invalidity, to the extent Defendants assert a detailed invalidity contention based in whole or in part on the cited article, SRI will provide a further response to this interrogatory at the time the Court's scheduling order has set for providing rebuttal contentions.

SECOND SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 15
(DECEMBER 15, 2005):

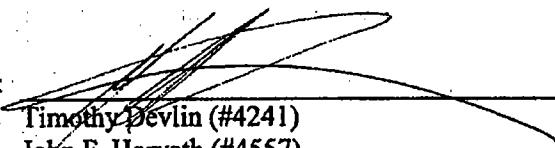
SRI incorporates by reference its previous response to Interrogatory No. 15 and its discussion of "*Next-generation Intrusion Detection Expert System (NIDES) A*

Summary," by Debra Anderson, Thane Frivold and Alfonso Valdes, Jan. 27, 1995, in section 6 of its Response to Symantec Invalidity Contentions.

Dated: December 15, 2005

FISH & RICHARDSON P.C.

By:


Timothy Devlin (#4241)
John F. Horvath (#4557)
FISH & RICHARDSON P.C.
919 N. Market St., Ste. 1100
P.O. Box 1114
Wilmington, DE 19889-1114
Telephone: (302) 652-5070
Facsimile: (302) 652-0607

Howard G. Pollack (CA Bar No. 162897)
Gina M. Steele (CA Bar No. 233379)
Katherine D. Prescott (CA Bar No. 215496)
Michael J. Curley (CA Bar No. 230343)
FISH & RICHARDSON P.C.
500 Arguello Street, Suite 500
Redwood City, California 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Attorneys for Plaintiff
SRI INTERNATIONAL, INC.

CERTIFICATE OF SERVICE

I hereby certify that on December 15, 2005, I served a copy of SRI INTERNATIONAL, INC.'S SUPPLEMENTAL RESPONSE TO INTERROGATORIES NO. 12 AND NO. 15 to the following in the manner indicated:

BY EMAIL & FEDERAL EXPRESS

Richard L. Horwitz
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
P.O. Box 951
Wilmington, DE 19899
Facsimile: (302) 658-1192

Attorneys for Defendant
INTERNET SECURITY SYSTEMS,
INC.

BY EMAIL & FEDERAL EXPRESS

Richard K. Herrmann Esq.
Morris James Hitchens & Williams
PNC Bank Center
222 Delaware Avenue, 10th Floor
P.O. Box 2306
Wilmington, DE 19899-2306
Facsimile: (302) 571-1750

Attorneys for Defendant
SYMANTEC CORPORATION

BY EMAIL & FEDERAL EXPRESS

Paul S. Grewal
Day Casebeer Madrid & Batchelder, LLP
20300 Stevens Creek Boulevard, Suite 400
Cupertino, California 95014

Attorney for Defendant
SYMANTEC CORPORATION

BY EMAIL & FEDERAL EXPRESS

Holmes Hawkins, III
King & Spalding
191 Peachtree Street, N.E.
Atlanta, GA 30303-1763

Attorneys for Defendant
INTERNET SECURITY SYSTEMS,
INC.

Katherine D. Prescott
Katherine D. Prescott

EXHIBIT XX

**EXHIBIT REDACTED
IN ITS ENTIRETY**

EXHIBIT YY

INTRUSION DETECTION

Rebecca Gurley Bace



Intrusion Detection

Rebecca Gurley Bace

Published by:

Macmillan Technical Publishing
201 West 103rd Street
Indianapolis, IN 46290 USA

Copyright ©2000 by Macmillan Technical Publishing

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

International Standard Book Number: 1-57870-185-6

Library of Congress Catalog Card Number: 99-63273-

03 02 01 00 7 6 5 4 3 2

Interpretation of the printing code: The rightmost double-digit number is the year of the book's printing; the rightmost single-digit number is the number of the book's printing. For example, the printing code 00-1 shows that the first printing of the book occurred in 2000.

*Composed in Galliard and MCPdigital by Macmillan Technical Publishing
Printed in the United States of America*

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Macmillan Technical Publishing cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

This book is designed to provide information about intrusion detection. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an as-is basis. The authors and Macmillan Technical Publishing shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

Feedback Information

At Macmillan Technical Publishing, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us at networktech@mcp.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

PUBLISHER

David Dwyer

EXECUTIVE EDITOR

Linda Ratts Engelman

MANAGING EDITOR

Gina Brown

PRODUCT MARKETING MANAGER

Stephanie Layton

ACQUISITIONS EDITOR

Karen Wachs

DEVELOPMENT EDITOR

Katherine Pendergast

PROJECT EDITOR

Alissa Cayton

COPY EDITOR

June Waldman

INDEXER

Larry Sweazy

ACQUISITIONS COORDINATOR

Jennifer Garrett

MANUFACTURING COORDINATOR

Chris Moos

BOOK DESIGNER

Louisa Kluczink

COVER DESIGNER

Aren Howell

COMPOSITORS

Scan Communications

Group, Inc.

Amy Parker

O V E R V I E W

Introduction	1
1 The History of Intrusion Detection	7
2 Concepts and Definitions	27
3 Information Sources	45
4 Analysis Schemes	79
5 Responses	121
6 Vulnerability Analysis: A Special Case	135
7 Technical Issues	155
8 Understanding the Real-World Challenge	173
9 Legal Issues	195
10 For Users	217
11 For Strategists	235
12 For Designers	255
13 Future Needs	275
Appendix A Glossary	289
Appendix B Bibliography	297
Appendix C Resources	315
Appendix D Checklist	321
Index	323

CONTENTS

<i>Introduction</i>	1
<i>Defining Intrusion Detection</i>	3
<i>By Way of Introduction</i>	4
1 The History of Intrusion Detection	7
<i>1.1 Audit: Setting the Stage for Intrusion Detection</i>	7
1.1.1 Differences between Financial and Security Audit	9
1.1.2 Audit as a Management Tool	9
1.1.3 EDP Audits and Early Computer Security	10
1.1.4 Audit and Military Models of Computer Security	11
<i>1.2 The Birth of Intrusion Detection</i>	12
1.2.1 Anderson and the Audit Reduction Problem	12
1.2.2 Denning, Neumann, and IDES	14
1.2.3 A Flurry of Systems through the 1980s	15
1.2.4 Integrating Host and Network-Based Intrusion Detection	21
1.2.5 The Advent of Commercial Products	23
<i>1.3 Conclusion</i>	24
<i>Endnotes</i>	25
2 Concepts and Definitions	27
<i>2.1 An Introduction to Intrusion Detection</i>	27
<i>2.2 Security Concepts</i>	28
2.2.1 A Cultural View of Computer and Network Security	28
2.2.2 Practical Definition of Computer Security	29
2.2.3 Formal Definition of Computer Security	29
2.2.4 Trust	30
2.2.5 Threat	30
2.2.6 Vulnerability	31
2.2.7 Security Policy	32
2.2.8 Other Elements of the System Security Infrastructure	33
2.2.9 How Security Problems Occur	35
<i>2.3 Intrusion Detection Concepts</i>	37
2.3.1 Architecture	37
2.3.2 Monitoring Strategy	38
2.3.3 Analysis Type	38
2.3.4 Timing	40
2.3.5 Goals of Detection	40
2.3.6 Control Issues	42

Table of Contents

xi

2.3.7 Determining Strategies for Intrusion Detection	43
2.4 Conclusion	43
Endnotes	44
3 Information Sources	45
3.1 The Organization of this Chapter	45
3.1.1 Which Source Is the Right Source?	46
3.1.2 Enduring Questions	46
3.2 Host-Based Information Sources	47
3.2.1 Operating System Audit Trails	47
3.2.2 Approaches to Structuring Audit Trails	48
3.2.3 Problems with Commercial Audit Systems	48
3.2.4 Pros and Cons of Operating System Audit Trails	49
3.2.5 Content of Audit Trails	49
3.2.6 Audit Reduction	57
3.2.7 System Logs	58
3.2.8 Applications Information	60
3.2.9 Target-Based Monitoring	65
3.3 Network-Based Information Sources	67
3.3.1 Why Network Sources?	67
3.3.2 Network Packets	67
3.3.3 TCP/IP Networks	68
3.3.4 Packet Capture	70
3.3.5 Network Devices	73
3.3.6 Out-of-Band Information Sources	73
3.4 Information from Other Security Products	74
3.4.1 An Example of a Security Product Data Source	74
3.4.2 Organization of Information Prior to Analysis	75
3.4.3 Other System Components as Data Sources	76
3.5 Conclusion	76
Endnotes	77
4 Analysis Schemes	79
4.1 Thinking About Intrusions	79
4.1.1 Defining Analysis	79
4.1.2 Goals	80
4.1.3 Supporting Goals	81
4.1.4 Detecting Intrusions	82
4.2 A Model for Intrusion Analysis	83
4.2.1 Constructing the Analyzer	84

4.2.2	Performing Analysis	88
4.2.3	Feedback and Refinement	89
4.3	<i>Techniques</i>	91
4.3.1	Misuse Detection	91
4.3.2	Anomaly Detection	100
4.3.3	Alternative Detection Schemes	110
4.4	<i>Conclusion</i>	117
	<i>Endnotes</i>	117
5	<i>Responses</i>	121
5.1	<i>Requirements for Responses</i>	121
5.1.1	Operational Environment	123
5.1.2	System Purpose and Priorities	123
5.1.3	Regulatory or Statutory Requirements	124
5.1.4	Conveying Expertise to Users	124
5.2	<i>Types of Responses</i>	125
5.2.1	Active Responses	125
5.2.2	Passive Responses	128
5.3	<i>Covering Tracks During Investigation</i>	130
5.3.1	Fail-Safe Considerations for Response Components	130
5.3.2	Handling False Alarms	130
5.3.3	Archive and Report	131
5.4	<i>Mapping Responses to Policy</i>	131
5.4.1	Immediate	132
5.4.2	Timely	132
5.4.3	Long-Term—Local	132
5.4.4	Long-Term—Global	133
5.5	<i>Conclusion</i>	133
	<i>Endnotes</i>	134
6	<i>Vulnerability Analysis: A Special Case</i>	135
6.1	<i>Vulnerability Analysis</i>	136
6.1.1	Rationale for Vulnerability Analysis	136
6.1.2	COPS—An Example of Vulnerability Analysis	136
6.1.3	Issues and Considerations	140
6.2	<i>Credentialed Approaches</i>	140
6.2.1	Definition of Credentialed Approaches	141
6.2.2	Determining Subjects for Credentialed Approaches	141
6.2.3	Strategy and Optimization of Credentialed Approaches	142

Table of Contents

xiii

6.3 Noncredentialed Approaches	144
6.3.1 Definition of Noncredentialed Approaches	144
6.3.2 Methods for Noncredentialed Vulnerability Analysis	144
6.3.3 Testing by Exploit	144
6.3.4 Inference Methods	145
6.3.5 A Historical Note	145
6.3.6 Architecture of SATAN	147
6.3.7 Fail-Safe Features	149
6.3.8 Issues Associated with SATAN	149
6.4 Password-Cracking	150
6.4.1 Concepts of Operation	150
6.4.2 Password Crackers as Vulnerability Analysis Tools	151
6.5 Strengths and Weaknesses of Vulnerability Analysis	151
6.5.1 Strengths of Credentialed Analysis Techniques	151
6.5.2 Strengths of Noncredentialed Analysis Techniques	152
6.5.3 Disadvantages	152
6.6 Conclusion	153
Endnotes	153
7 Technical Issues	155
7.1 Scalability	155
7.1.1 Scaling over Time	155
7.1.2 Scaling over Space	156
7.1.3 Case Study—GrIDS	157
7.2 Management	157
7.2.1 Network Management	158
7.2.2 Sensor Control	159
7.2.3 Investigative Support	159
7.2.4 Performance Loads	160
7.3 Reliability	160
7.3.1 Reliability of Information Sources	161
7.3.2 Reliability of Analysis Engines	162
7.3.3 Reliability of Response Mechanisms	163
7.3.4 Reliability of Communications Links	164
7.4 Analysis Issues	165
7.4.1 Training Sets for AI-Based Detectors	165
7.4.2 False Positives/Negatives in Anomaly Detection	165
7.4.3 Trends Analysis	166
7.4.4 Composition of Policies	166

7.5 Interoperability	167
7.5.1 CIDF/CRISIS Effort	169
7.5.2 Audit Trail Standards	169
7.6 Integration	171
7.7 User Interfaces	171
7.8 Conclusion	172
<i>Endnotes</i>	172
8 Understanding the Real-World Challenge	173
8.1 The Roots of Security Problems	173
8.1.1 Problems in Design and Development	174
8.1.2 Problems in Management	178
8.1.3 Problems in Trust	181
8.2 Through a Hacker's Eyes	185
8.2.1 Identifying a Victim	185
8.2.2 Casing the Joint	186
8.2.3 Gaining Access	186
8.2.4 Executing the Attack	187
8.3 Security versus Traditional Engineering	191
8.3.1 Traditional Engineering	191
8.3.2 Security Engineering	191
8.3.3 Rules of Thumb	192
8.4 Rules for Intrusion Detection Systems	192
8.5 Conclusion	194
<i>Endnotes</i>	194
9 Legal Issues	195
9.1 Law for Geeks	196
9.1.1 Legal Systems	197
9.1.2 Legislation	198
9.1.3 Civil Litigation/Tort Law	199
9.1.4 Complications in Applying Law to Cyberspace	201
9.2 Rules of Evidence	203
9.2.1 Types of Evidence	203
9.2.2 Admissibility of Evidence	204
9.2.3 Restrictions and Exceptions	205
9.2.4 Provisions for Handling Evidence	205
9.2.5 Rules of Evidence as Applied to System Logs and Audit Trails	206
9.3 Laws Relating to Monitoring Activity	207
9.3.1 When a System Administrator Monitors a System	207

Table of Contents

xv

9.3.2 When Law Enforcement Agents Monitor a System	208
9.3.3 Notification of Monitoring	208
9.4 What Real Cases Have Taught Us	208
9.4.1 The Mitnick Case	209
9.4.2 The Rome Lab Case	212
9.4.3 Lessons Learned	214
9.5 Conclusion	215
<i>Endnotes</i>	216
10 For Users	217
10.1 Determining Your Requirements	217
10.1.1 Your System Environment	217
10.1.2 Goals and Objectives	218
10.1.3 Reviewing Your Policy	218
10.1.4 Requirements and Constraints	219
10.2 Making Sense of Products	220
10.2.1 Understanding the Problem Space	220
10.2.2 Is the Product Scalable?	221
10.2.3 How Did You Test This?	221
10.2.4 Is This Product a Tool or Is It an Application?	222
10.2.5 Buzzwords versus Wisdom	223
10.2.6 Anticipated Life of Product	224
10.2.7 Training Support	224
10.2.8 Prioritized Goals of Product	224
10.2.9 Product Differentiation	225
10.3 Mapping Policy to Configurations	225
10.3.1 Converting Policy to Rules	225
10.3.2 Subject-Objects to Real World	226
10.3.3 Monitoring Policy versus Security Policy	227
10.3.4 Testing Assertions	227
10.4 Show Time! Incident Handling and Investigation	227
10.4.1 Scout's Honor	228
10.4.2 Best Practices	228
10.4.3 When the Balloon Goes Up	229
10.4.4 Dealing with Law Enforcement	230
10.4.5 Expectations	231
10.4.6 Damage Control	231
10.4.7 Dealing with Witch Hunts	232
10.5 Conclusion	232
<i>Endnotes</i>	233

<i>For Strategists</i>	235
11.1 <i>Building a Case for Security</i>	235
11.1.1 Assembling Information	236
11.1.2 What Is the Organization Trying to Accomplish?	236
11.1.3 How Does Security Fit Into Overall Business Goals?	236
11.1.4 Where Does Information Security Fit Into the Corporate Risk-Management Program?	237
11.1.5 What Do We Need to Secure the System?	238
11.1.6 Finding Allies	239
11.1.7 Overcoming Management Resistance	241
11.2 <i>Defining Requirements for IDS</i>	242
11.2.1 Revisiting Goals and Objectives	242
11.2.2 What Are the Threats?	242
11.2.3 What Are Our Limitations?	243
11.2.4 Considerations in Adopting Intrusion Detection and System Monitoring	243
11.3 <i>Marketing Hype versus Real Solutions</i>	244
11.3.1 What Product Is Best Fitted to Us and Our Goals?	244
11.3.2 How Painful Is This Product to Install?	245
11.3.3 How Painful Is This Product to Run?	245
11.3.4 What Are the Expectations of the Personnel?	246
11.3.5 Who Was the Dream Customer for Whom This Product Was Designed?	246
11.4 <i>Integrating Security Into a Legacy Environment</i>	246
11.4.1 Assessing the Existing Systems	247
11.4.2 Leveraging Investments in Security	247
11.4.3 Dealing with "Wetware"—the Humans in the System	248
11.4.4 Handling Conflicts	249
11.5 <i>Dealing with the Effects of Corporate Transitions</i>	250
11.5.1 Mergers and Acquisitions	250
11.5.2 Strategic Partners	250
11.5.3 Globalization	251
11.5.4 Expansion and Contraction	251
11.5.5 Going from Private to Public	252
11.6 <i>Conclusion</i>	252
<i>Endnotes</i>	253

Table of Contents

xvii

<i>For Designers</i>	255
<i>12.1 Requirements</i>	256
12.1.1 Good versus Great Intrusion Detection	256
12.1.2 Different Approaches to Security	258
12.1.3 Policies—One Size Does Not Fit All	260
<i>12.2 Security Design Principles</i>	262
12.2.1 Economy of Mechanism	262
12.2.2 Fail-Safe Defaults	263
12.2.3 Complete Mediation	263
12.2.4 Open Design	263
12.2.5 Separation of Privilege	264
12.2.6 Least Privilege	264
12.2.7 Least Common Mechanism	265
12.2.8 Psychological Acceptability	265
<i>12.3 Surviving the Design Process</i>	265
12.3.1 Establishing Priorities	265
12.3.2 On Threat Curmudgeons	266
12.3.3 Striking and Maintaining Balance	267
<i>12.4 Painting the Bull's Eye</i>	268
12.4.1 Gauging Success	268
12.4.2 False Starts	269
12.4.3 Testing Approaches	269
12.4.4 Measuring Network-Based Performance	270
<i>12.5 Advice from the Trenches</i>	271
12.5.1 Use Good Engineering Practices	271
12.5.2 Secure Sensors	272
12.5.3 Pay Attention to Correct Reassembly	272
12.5.4 Don't Underestimate Hardware Needs	272
12.5.5 Don't Expect Trusted Sources of Attack Data	272
12.5.6 Think Through Countermeasures	273
12.5.7 No Support for Forensics	273
12.5.8 Support Modern Security Features	273
<i>12.6 Conclusion</i>	273
<i>Endnotes</i>	274
<i>Future Needs</i>	275
<i>13.1 Future Trends in Society</i>	276
13.1.1 Global Villages and Marketplaces	276
13.1.2 Privacy as an Economic Driver	276
13.1.3 A Different Kind of War	277

xviii | Intrusion Detection

13.1.4	Sovereignty	277
13.2	<i>Future Trends in Technology</i>	277
13.2.1	Changes in the Network Fabric	277
13.2.2	Open Source Software	278
13.2.3	Advances in Wireless Networking	278
13.2.4	Ubiquitous Computing	279
13.3	<i>Future Trends in Security</i>	279
13.3.1	Management	279
13.3.2	Privacy-Sparing Security	281
13.3.3	Information Quality versus Access Control	282
13.3.4	Crypto, Crypto Everywhere . . .	282
13.3.5	The Erosion of Perimeters	282
13.3.6	Liability Transfer versus Trust Management	283
13.4	<i>A Vision for Intrusion Detection</i>	283
13.4.1	Capabilities	283
13.4.2	Highly Distributed Architectures	284
13.4.3	911 for Security Management	285
13.4.4	Ubiquitous Information Sources	285
13.4.5	Silicon Guards	285
13.4.6	Emphasis on Service, Not Product	286
13.5	<i>Conclusion</i>	286
<i>Endnotes</i>		287
Appendix A	<i>Glossary</i>	289
Appendix B	<i>Bibliography</i>	297
Appendix C	<i>Resources</i>	315
<i>Books</i>		315
Intrusion Detection and Associated Technologies		315
Security References and Textbooks		315
Information Warfare, Critical Systems, and National Policy		316
Introduction to Computer and Network Security		316
Cryptography		316
Firewalls		316
War Stories		317
Specific Application Venues		317
Cybercrime and Law Enforcement		317
For Fun		317

Table of Contents xix

<i>WWW Resources</i>	317
Security Portals	318
Vulnerability Information Sources	318
Organizations	318
Government Sites	319
Academic Sites	319
Commercial Products, Services, and Research	319
Miscellaneous Intrusion Detection References	320
<i>Appendix D Checklist</i>	321
<i>Index</i>	323

CHAPTER 1 The History of Intrusion Detection

19

runs on a Sybase database management system, using some of Sybase's internal triggers and other features.

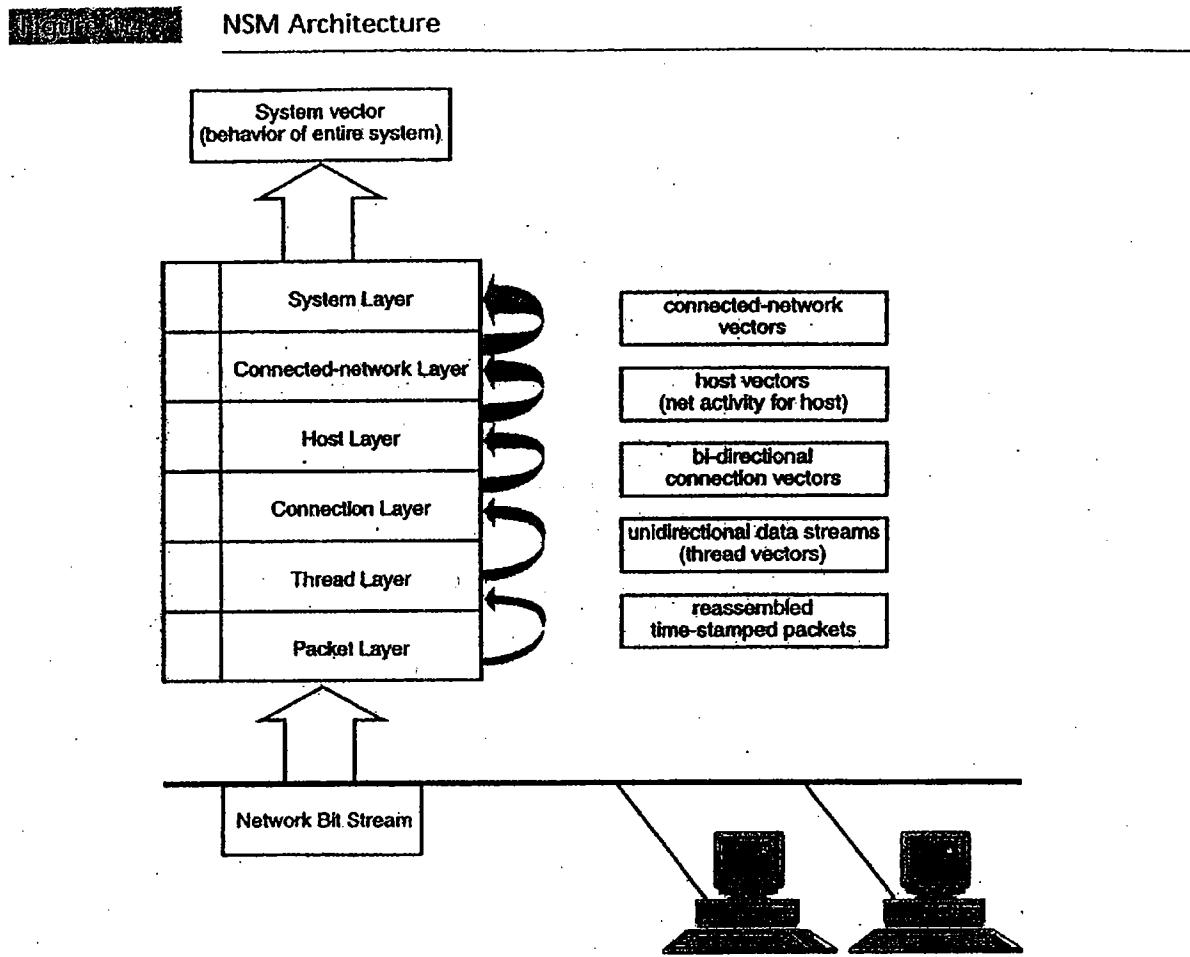
NADIR remains one of the most successful and durable intrusion detection systems of the 1980s and has been extended to monitor systems beyond the ICN at Los Alamos. NADIR continues to monitor the ICN at the time of this publication, and the team continues to modify the system to accommodate new threats and target systems. The principal architect for NADIR is Kathleen Jackson.

1.2.3.6 NSM

The Network System Monitor (NSM) was developed at the University of California at Davis to run on a Sun UNIX workstation. It represented the first foray into monitoring network traffic and using that traffic as the primary data source. Before this time, most intrusion detection systems consumed information from operating system audit trails or keystroke monitors. The general architecture of the NSM is still reflected in many commercial intrusion detection products at the time of this publication. The NSM functioned by doing the following:

- Placing the system's Ethernet network interface card into promiscuous mode (in which each network frame generates an interrupt, thereby allowing the monitoring system to listen to all traffic, not just those packets addressed to the system)
- Capturing network packets
- Parsing the protocol to allow extraction of pertinent features as shown in Figure 1.4
- Using a matrix-based approach to archive and analyze the features, both for statistical variances from normal behavior and for violations of pre-established rules

NSM was a significant milestone in intrusion detection research because it was the first attempt to extend intrusion detection to heterogeneous network environments. It was also one of the first intrusion detection systems to run on an operational system (the computer science department local area network at UC Davis). In a widely cited, two-month test of NSM, it monitored more than 111,000 connections on the network segment, correctly identifying more than 300 of them as intrusions. The system administrators for the network discovered less than one percent of these intrusions. This test emphasized the need for and the effectiveness of intrusion detection systems as part of the protection suite. Principal architects for NSM were Karl Levitt, Todd Heberlein, and Biswanath Mukherjee of the University of California at Davis.¹⁵



1.2.3.7 Wisdom and Sense

Wisdom and Sense¹⁶ was an anomaly detection system developed by the Safeguards and Security Group at Los Alamos National Laboratory in partnership with Oak Ridge National Laboratory. Wisdom and Sense was the second pass at an intrusion detection system for mainframes (the initial system, called ALAP, was fielded by the U.S. Department of Energy in several of the department's facilities). Wisdom and Sense operated on a UNIX platform and analyzed audit data from Digital Equipment Corporation VAX/VMS systems. Wisdom and Sense performed statistical, rule-based analyses that were quite different from other systems of the time. The system used *nonparametric techniques* (which are statistical techniques that make no assumptions about the distribution of the data) to derive its own rulebase from archival audit data. Wisdom and Sense then compared subsequent activity to this rulebase, looking for exceptions. The rulebase was structured into

CERTIFICATE OF SERVICE

I hereby certify that on the 19th day of July, 2006, I electronically filed the foregoing document, **REDACTED VERSION OF DECLARATION OF GEOFFREY M. GODFREY IN SUPPORT OF DEFENDANTS' JOINT REPLY MOTION FOR SUMMARY JUDGMENT REGARDING INVALIDITY**, with the Clerk of the Court using CM/ECF which will send notification of such filing to the following:

John F. Horvath, Esq.
Fish & Richardson, P.C.
919 North Market Street, Suite 1100
Wilmington, DE 19801

Richard L. Horwitz, Esq.
David E. Moore, Esq.
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
Wilmington, DE 19801

Additionally, I hereby certify that on the 19th day of July, 2006, the foregoing document was served via email on the following non-registered participants:

Howard G. Pollack, Esq.
Michael J. Curley, Esq.
Fish & Richardson
500 Arguello Street, Suite 500
Redwood City, CA 94063
650.839.5070

Holmes Hawkins, III, Esq.
King & Spalding
191 Peachtree Street
Atlanta, GA 30303
404.572.4600

Theresa Moehlman, Esq.
King & Spalding LLP
1185 Avenue of the Americas
New York, NY 10036-4003
212.556.2100

/s/ Richard K. Herrmann

Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
Morris, James, Hitchens & Williams LLP
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
(302) 888-6800
rherrmann@morrisjames.com

Counsel for Symantec Corporation